УДК 342.95:004:343.3/7

В. В. МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ЩОДО ЗАРУБІЖНОГО ДОСВІДУ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Досліджено особливості злочинів у сфері інформаційно-телекомунікаційних технологій, звернуто увагу на основні проблеми щодо їх виявлення, розкриття та розслідування. Розкрито напрямки міжнародної взаємодії у сфері протидії кіберзлочинності, що базуються на міжнародних нормативно-правових актах. Висвітлено певний зарубіжний досвід організації діяльності підрозділів поліції та нормативного регулювання у Співдружності націй та Європейському Союзі в означеній сфері. Наголошено на необхідності вивчення досвіду зарубіжних країн щодо організації діяльності підрозділів боротьби з кіберзлочинністю. Проаналізовано досвід діяльності поліції Канади в цьому напрямку. Виділено рівні взаємодії оперативних підрозділів внутрішніх справ з метою оперативного документування злочинів у сфері інформаційно-телекомунікаційних технологій та види співробітництва органів внутрішніх справ з правоохоронними органами інших держав.
Зауважено, що удосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні має відбуватися з урахуванням національних особливостей на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн.

Ключові слова: *інформатизація суспільства, злочини у сфері інформаційно-телекомунікаційних технологій, протидія кіберзлочинності, міжнародний досвід, поліція, Канада, органи внутрішніх справ, рівні взаємодії, види співробітництва.*

Markov, V.V. (2015), "On the issue of foreign experience in combating cybercrime" ["Do pytannia shchodo zarubizhnoho dosvidu protydii kiberzlochynnosti"], *Pravo i Bezpeka*, No. 2, pp. 107–113.

Постановка проблеми. Серед сучасних тенденцій розвитку суспільства слід відзначити глобальну інформатизацію практично всіх сфер життєдіяльності людини, включаючи економіку, державне управління, науку, мистецтво. Загальна інформатизація є основною ознакою переходу цивілізованого світу до стану технологічно нового, інформаційного суспільства. Невпинно зростають темпи розвитку цифрової економіки, що в декілька разів перевищують показники всіх інших галузей виробництва [1, с. 167]. В умовах глобальної інформатизації змінюється характер формування сучасних правовідносин у сфері розповсюдження інформації, сутність, зміст, роль і місце організаційно-правових основ захисту інформації, у тому числі з обмеженим доступом до певних видів інформації, зокрема правоохоронної діяльності і забезпечення суспільного порядку [2, с. 5–6].

Однак становлення інформаційного суспільства в Україні стримується низкою проблем нормативно-правового та організаційного векторів [3]. У період глобалізації швидкий розвиток інформаційних технологій, нових систем комунікацій і комп'ютерних мереж супроводжується зловживанням цими технологіями зі злочинною метою. Саме тому питання вивчення та запозичення міжнародного досвіду провідних країн світу в сфері державної діяльності щодо адміністративно-правових механізмів регулювання захисту інформації у сучасних умовах, протидії кіберзлочинності є актуальним і для забезпечення стратегічних намірів України щодо європейської і євроатлантичної інтеграції [2, с. 5–6].

Стан дослідження. Окремі аспекти розвитку та становлення інформаційних відносин, питання здійснення протидії кіберзлочинності розглядались провідними вітчизняними науковцями М. О. Будаковим, В. М. Бутузовим, М. М. Галамбою, Р. А. Калюжним, В. В. Коваленко, Я. Ю. Кондратьєвим, Б. А. Кормичем, Ю. Є. Максименко, А. І. Марущаком, Г. В. Новицьким та іноземними фахівцями А. Робертом, К. Осакве, Т. Блентаном, Д. Банісаром та ін. Однак необхідність подальшого наукового пошуку обґрунтовується наявністю прогалин у національному законодавстві щодо регламентації адміністративно-правової протидії кіберзлочинності в Україні. На цьому напрямку важливим є вивчення зарубіжного досвіду протидії кіберзлочинності як окремих країн, так і міжнародної спільноти, що і є **метою** статті.

Виклад основного матеріалу. Так, Ю. Є. Максименко зазначає, що становлення інформаційного суспільства має як безсумнівні позитивні, так і певні негативні наслідки. З одного боку, пришвидшилася передача інформації великого обсягу, прискорились її обробка та впровадження. З іншого – серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо.

Перетворення суспільства в інформаційне змінив статус інформації. На сьогодні вона може бути як засобом забезпечення безпеки, так і загрозою та небезпекою [4, с. 1].

Безперечно, на сучасному етапі розвитку людського суспільства важливим стратегічним ресурсом, що потребує охорони, є інформація, яка містить надзвичайно широкий спектр зведень: від простих даних про громадян країни до стратегічних державних програм. Тому ці дані все частіше стають предметом злочинних зазіхань. Комплексне і широкомасштабне використання інформаційних технологій на основі персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних систем забезпечило людству вихід на новий етап свого розвитку – етап інформаційного суспільства. Як наслідок – поява нового виду злочинності – комп'ютерної, або кіберзлочинності.

Одним із можливих підходів до боротьби з кіберзлочинністю у транснаціональному аспекті і розвитку міжнародної співпраці є вироблення і стандартизація відповідної нормативно-правової бази. На міжнародному рівні першими документами у цій сфері стали Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001 р. [5], та Додатковий протокол до Конвенції, направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського і ксенофобського характеру від 28 січня 2003 р. [6]. Прийняття цих актів ознаменувало закладення правового фундаменту у сферу захисту свободи, безпеки і прав людини в мережі Інтернет не тільки на регіональному рівні, оскільки Конвенція відкрита для підписання державами, які не є членами Ради Європи [7].

Для багатьох країн, зокрема і для України, кіберзлочинність є достатньо актуальним явищем, породженим широким впровадженням в економічні процеси сучасних інформаційних та телекомунікаційних технологій.

Характерними особливостями злочинів у сфері інформаційно-телекомунікаційних технологій є:

– необхідність широкого застосування спеціальних знань при виявленні та фіксації слідів злочину в електронній формі;

– організованість та транскордонність (широкі міжрегіональні та міжнародні зв'язки);

– висока латентність, спричинена небажанням приватного сектора інформувати про такі злочини через недовіру до потенційних можливостей правоохоронних органів та небажанням визнати слабкі місця своїх систем безпеки;

– високий рівень технічного забезпечення правопорушників.

До основних проблем виявлення, розкриття та розслідування «транскордонних» злочинів з використанням глобальної мережі Інтернет слід віднести територіальну розподіленість слідів злочину та зберігання їх протягом невеликого проміжку часу. Правоохоронцям іноді важко окреслити території, де здійснюються сучасні злочини. У злочинців у мережі Інтернет великий ступінь анонімності, а інформація, що зберігається в комп'ютерних системах, має короткостроковий характер.

Враховуючи особливості злочинів у сфері інформаційно-комунікаційних технологій, важливе значення для результативності їх оперативного документування має взаємодія оперативного підрозділу внутрішніх справ на всіх рівнях, у тому числі із представниками правоохоронних органів інших країн [8, с. 518–519]. Для покращення співпраці Конвенцією передбачено створення сторонами на національному рівні органу для здійснення контактів цілодобово з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає в себе сприяння або, якщо це дозволяється внутрішньодержавним законодавством і практикою, пряме: a) надання технічних порад; b) збереження даних відповідно до статей 29 («Термінове збереження комп'ютерних даних, які зберігаються») і 30 («Термінове розкриття збережених даних про рух інформації»); c) збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних (ст. 35) [5].

Конвенцією встановлені також обов'язкові вимоги для врахування у законодавстві країн, які приєдналися:

– надання органам дізнання та слідства повноважень щодо видачі обов'язкових до виконання приписів про термінове фіксування та подальше зберігання комп'ютерних даних, необхідних для розкриття злочину (ч. 1 ст. 16, ст. 17);

– збереження провайдерськими установами даних про трафік інформації на термін до 90 днів з можливістю подальшого продовження цього строку (ч. 2 ст. 16);

– встановлення для суб'єктів, які зберігають комп'ютерні дані, зобов'язання не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом періоду, що визначається законодавством держави (ч. 3 ст. 16, ч. 3 ст. 20, ч. 3 ст. 21) [5].

Питання боротьби з кіберзлочинністю знаходяться й у центрі уваги органів та інституцій Організації Об'єднаних Націй, зокрема Генеральної Асамблеї (A/RES 63/195), Економічної і Соціальної Ради (рез. 2009/22), Комісії з попередження злочинності і кримінального правосуддя (док. E/ CN.15/2009/15), конгресів ООН з попередження злочинності і кримінального правосуддя, рішення яких потребують розробки шляхів і засобів їх вирішення [7, с. 195].

У ряді міждержавних нормативно-правових актів [6; 9; 10] визнано, що кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремої держави, а й загрожує людству в цілому. Саме тому цій проблемі приділяється значна увага у багатьох державах.

Проаналізувавши досвід роботи поліції багатьох країн світу в сфері протидії кіберзлочинності, слід відзначити, що цей напрямок забезпечується такими основними шляхами, як покладення додаткових функцій на існуючі підрозділи поліції або створення спеціальних підрозділів.

Створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності практикується в багатьох країнах світу, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції та ін.

Серед основних функцій цих підрозділів виділяють:

– моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;

– здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців;

– розслідування кіберзлочинів, надання методичної та практичної допомоги іншим галузевим службам і правоохоронним органам у межах своєї компетенції;

– накопичення, узагальнення та аналіз інформації про кіберзлочинність;

– профілактику кіберзлочинів за допомогою громадськості та засобів масової інформації;

– навчання працівників поліції.

Деякі зі спеціальних підрозділів поліції у сфері протидії кіберзлочинності (або їх ще називають спеціальними підрозділами щодо протидії злочинам з використанням інформаційних технологій) виконують ще й додаткові функції:

– розкриття кіберзлочинів;

– профілактики та нагляду за телекомунікаційними послугами;

– експертного дослідження доказів на електронних носіях;

– створення відповідної бази даних щодо злочинів у сфері кіберпростору та постійного її оновлення;

– надання послуг банкам щодо захисту персональної інформації клієнтів тощо.

Наприклад, в Індії підрозділи з розслідування кіберзлочинів для їх розкриття можуть залучати професійних хакерів.

Слід зазначити, що під час розслідування кіберзлочинів значну увагу приділяють допомозі постраждалому у відновленні пошкодженої або втраченої інформації, вживають всі необхідні заходи для збереження доказів у справі [11, с. 193].

Крім того, в останні роки у різних регіонах світу було застосовано низку своїх підходів для боротьби з кіберзлочинністю. Так, у 2002 році Співдружністю націй був розроблений типовий закон про комп'ютерні та пов'язані з комп'ютерами злочинами, метою якого є удосконалення законодавчих норм держав – членів Співдружності в галузі боротьби з кіберзлочинністю і поглиблення міжнародної співпраці. За відсутності цього договору, для розвитку транскордонної співпраці у цій галузі, членам Співтовариства націй необхідно було б укласти між собою низку двосторонніх договорів, які б набагато ускладнили процедуру співпраці. Типовий закон містить, зокрема, положення про міжнародну співпрацю. Оскільки він має регіональний характер, то його положення стосуються лише держав – членів Співдружності (п. 20).

Європейським Союзом докладено зусиль з узгодження законодавства щодо кіберзлочинності, яке діє на території держав – членів

організації. Для цього були прийняті, зокрема: директива № 2000/31/ЄС Європейського парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, таких, як електронна торгівля на внутрішньому ринку; рамкове рішення Ради Європейського Союзу 2000/41/ЈНА про боротьбу з шахрайством і фальсифікацією безготівкових платіжних засобів; рамкове рішення Ради Європейського Союзу 204/68/ЈНА про боротьбу із сексуальною експлуатацією тощо (п. 20–21) [12].

Необхідно зазначити, що на шляху удосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні ми маємо вивчати позитивний досвід діяльності правоохоронних органів інших країн в цьому напрямку.

Зокрема, одним із важливих напрямків діяльності поліції Канади є боротьба з комп'ютерними і телекомунікаційними злочинами, розслідуванням яких займається підрозділ Королівської канадської кінної поліції (федеральної поліції, КККП) з боротьби з комп'ютерною злочинністю, опираючись на дані канадського поліцейського інформаційного центру та співпрацюючи з іншими країнами. Діяльність підрозділу направлена на розслідування та розкриття злочинів, пов'язаних із комп'ютерами і телекомунікаціями. Секція захисту інформаційних технологій забезпечує захист федеральних державних комп'ютерних центрів, приватного сектора, дає консультації, готує персонал для роботи зі здійснення комп'ютерного захисту. Співробітники підрозділу допомагають поліцейським у проведенні розслідувань злочинів, пов'язаних із комп'ютерними системами.

Враховуючи, що інформаційна система дозволяє передавати повідомлення від одного терміналу до іншого майже негайно, у Канаді діє близько 2500 точок доступу, до яких входять близько 1285 федеральних і провінційних поліцейських відділень. 1180 підрозділів спеціалізованих відділів КККП підключені до ліній системи [13].

Безперечно, цей напрямок діяльності поліції є важливим, оскільки економічні втрати вже досягли широких масштабів, деякі злочинці діють на міжнародному рівні організованою групою. Водночас слід визнати, що канадське законодавство щодо визначення комп'ютерної злочинності потребує вдосконалення. Враховуючи, що завдання, які стоять перед підрозділами поліції з боротьби з комп'ютерною злочинністю, носять міжнародний характер і не є специфічними для Канади, вони активно співпрацюють з іншими країнами та Інтерполом з метою вдосконалення законодавства у цьому напрямку.

Розкриття комп'ютерних злочинів являє собою складне завдання, у першу чергу через фактор часу. Оскільки передача даних може бути виконана майже миттєво, часто буває даремно шукати будь-які докази, що підтверджують порушення міжнародного законодавства. За даними КККП, на сьогодні безліч комп'ютерних злочинів здійснюється дітьми, які не досягли дванадцятирічного віку. Згідно з кримінальним кодексом Канади для встановлення кримінальної відповідальності необхідно довести несанкціоноване використання комп'ютерної системи та намір особи заподіяти своїми діями шкоду. Такий підхід потребує чіткого встановлення параметрів доступу до комп'ютерної техніки з метою попередження порушень. Необхідно враховувати дані про осіб, параметри доступу з урахуванням обмежень, можливість службовців «експериментувати» з програмами. Кваліфіковану консультацію щодо можливої неправомірної поведінки в цьому напрямку може надати міністерство юстиції чи відповідний підрозділ КККП.

Слід зазначити, що методика розслідування випадків несанкціонованого дистанційного доступу до комп'ютерних мереж технічно складна, ними займаються спеціалізовані поліцейські підрозділи. З огляду на небезпеку комп'ютерної злочинності, тенденцію її розвитку та впливу на світове співтовариство у межах ООН регулярно проводяться симпозіуми з профілактики і припинення комп'ютерної злочинності. Як один із напрямків фахівці відзначають програмні методи захисту інформації в комп'ютерних системах колективного користування шляхом удосконалення системи автоматичного контролю. На попередження та зменшення злочинів щодо незаконного використання телекомунікаційних систем на міжпровінційному, державному і міжнародному рівних спрямовані дії та управління боротьби з економічними злочинами. Допомагає поліцейським підрозділам Інформаційний центр.

Поліцейська діяльність щодо попередження та розкриття діянь, пов'язаних із кіберзлочинністю, спрямована і на різнобічний розвиток відносин з якомога більшим суспільним колом через засоби масової інформації, консультативні зустрічі з представниками громадськості, взаємовідносини з різноманітними органами влади і управління, громадськими організаціями, окремими громадянами.

Таким чином, поліція є важливим партнером у співтоваристві відомств, що займаються

боротьбою зі злочинністю, в тому числі кіберзлочинністю, забезпеченням дотримання прав людини, забезпеченням захисту федеральних державних комп'ютерних центрів, приватного сектора [13].

Ефективна боротьба із комп'ютерною злочинністю вимагає більш дієвого та ефективно функціонуючого співробітництва правоохоронних органів різних країн, у тому числі в межах Інтерполу.

Погоджуємось з думкою вчених (як, наприклад, В. В. Коряк, В. Р. Сливенко) щодо визначення взаємодії в органах внутрішніх справ як узгодженої в часі, методах і засобах діяльності підрозділів (або працівників), не пов'язаних між собою прямим підпорядкуванням, для реалізації загальних цілей і вирішення завдань.

Враховуючи особливості злочинів у сфері інформаційно-комунікаційних технологій, важливе значення для результативності їх оперативного документування має взаємодія оперативного підрозділу внутрішніх справ на всіх рівнях:

1) внутрішньовідомчому – з іншими оперативними підрозділами кримінальної міліції, науково-дослідними експертно-криміналістичними центрами та слідчими підрозділами;

2) внутрішньодержавному – з іншими правоохоронними органами України, трудовими колективами, громадськими організаціями й населенням;

3) міжнародному – з правоохоронними органами інших країн.

Так, основними видами співробітництва органів внутрішніх справ України з правоохоронними органами інших держав є:

– обмін відомостями оперативно-розшукового характеру;

– надсилання правової допомоги у кримінальних справах;

– виїзд членів слідчо-оперативних груп за кордон для присутності під час виконання слідчих дій та оперативно-розшукових заходів;

– виїзд для обміну інформацією оперативно-розшукового характеру;

– виїзд за кордон для присутності під час проведення слідчих та інших дій у межах надання правової допомоги;

– виїзд для конвоювання розшуканих і затриманих за кордоном осіб;

– виїзд працівників прикордонних ГУМВС, УМВС України в сусідні регіони суміжних держав в оперативно-розшукових справах;

– прибуття працівників правоохоронних органів іноземних держав в Україну для проведення слідчих і оперативно-розшукових дій [8, с. 523–535].

Підводячи підсумки, зазначимо, що сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу, до глобального інформаційного простору. Саме тому ми маємо використовувати досвід країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки [14, с. 225], оскільки вона є невід'ємним напрямком побудови інформаційного суспільства, розвиток якого повинен йти не лише через нарощування технологічних можливостей здійснення інформаційного обміну, а й через глибоке усвідомлення всіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо захисту інформаційних ресурсів та забезпечення безпеки держави, у тому числі враховуючи зарубіжний досвід протидії кіберзлочинності в сфері адміністративно-правового забезпечення. Тільки скоординованими зусиллями організацій та відомств незалежно від форм власності, шляхом налагодження міжнародного співробітництва, використовуючи сучасні технології захисту інформації можна отримати переваги не лише електронного бізнесу, а й інформаційної революції в цілому, не забуваючи про інформаційну безпеку держави та окремих громадян.

Слід зазначити, що удосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні має відбуватися з урахуванням національних культурно-історичних, соціально-економічних особливостей країни на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн у сфері боротьби з кіберзлочинністю з метою оптимального входження у європейське та світове правове поле.

Список використаних джерел

1. Бойченко О. В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія / О. В. Бойченко ; Крим. юрид. ін-т ОДУВС. – Сімферополь : Сімферопол. міська друк., 2009. – 288 с.

2. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. / В. С. Сідак, В. Ю. Артемов. – Київ : КНТ, 2007. – 160 с.

3. Бойченко О. В. Угрозы информационных ресурсов государственного самоуправления / О. В. Бойченко // Материалы Международной научно-практической конференции «Проблемы и особенности влияния

международной информации на экономические и общественно-политические процессы». – Симферополь : ИСВА МСУ, 2007. – С. 39–41.

4. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. … канд. юрид. наук : 12.00.01 / Максименко Юлія Євгеніївна. – Київ, 2007. – 20 с.

5. Конвенція [Ради Європи] про кіберзлочинність : від 23 листоп. 2001 р. ; ратиф. Україною 7 верес. 2005 р. // Офіційний вісник України. – 2007. – № 65. – Ст. 2535.

6. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : від 28 січ. 2003 р. ; ратиф. Україною 21 серп. 2006 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_687.

7. Сироїд Т. Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю / Сироїд Тетяна Леонідівна // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. – Харків : Права людини, 2014. – С. 194–196.

8. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – Київ : Скіф, 2012. – 728 с.

9. Конвенція [ООН] проти транснаціональної організованої злочинності : прийн. резолюцією 55/25 Ген. Асамблеї від 15 листоп. 2000 р. ; ратиф. із застереженнями і заявами законом України від 4 лют. 2004 р. № 1433-15 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/995_789.

10. Конвенция об информационном и правовом сотрудничестве, касающемся «Информационных общественных услуг» : ETS № 180 от 4 окт. 2001 г. – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_559.

11. Сень Р. Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів / Руслан Юрійович Сень // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. – Харків : Права людини, 2014. – С. 192–194.

12. Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию (Сальвадор, Бразилия, 12–19 апр. 2010г.) : A / CJNF.213/1 [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/conf/crimecongress2010/.

13. Варунц Л. Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні : дис. канд. юрид. наук : 12.00.07 / Варунц Лариса Дмитрівна. – Дніпропетровськ, 2012. – 203 с.

14. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – Київ : КНТ, 2006. – 280 с. – (Серія: Нац. і міжнар. безпека).

Надійшла до редколегії 03.08.2015

МАРКОВ В. В. К ВОПРОСУ О ЗАРУБЕЖНОМ ОПЫТЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Исследованы особенности преступлений в сфере информационно-телекоммуникационных технологий, обращено внимание на основные проблемы их выявления, раскрытия и расследования. Раскрыты направления международного взаимодействия в сфере противодействия киберпреступности, основанные на международных нормативно-правовых актах. Освещен определенный зарубежный опыт организации деятельности подразделений полиции и нормативного регулирования в Содружестве наций и Европейском Союзе в указанной сфере. Отмечена необходимость изучения опыта зарубежных стран по организации деятельности подразделений по борьбе с киберпреступностью. Проанализирован опыт деятельности полиции Канады в этом направлении. Выделены уровни взаимодействия оперативных подразделений внутренних дел с целью оперативного документирования преступлений в сфере информационно-телекоммуникационных технологий и виды сотрудничества органов внутренних дел с правоохранительными органами других государств.

Отмечено, что совершенствование административно-правового обеспечения противодействия киберпреступности в Украине должно происходить с учетом национальных особенностей на основании детального научного анализа международного законодательства и опыта других стран.

Ключевые слова: *информатизация общества, преступления в сфере информационно-телекоммуникационных технологий, противодействие киберпреступности, международный опыт, полиция, Канада, органы внутренних дел, уровни взаимодействия, виды сотрудничества.*

MARKOV V. V. ON THE ISSUE OF FOREIGN EXPERIENCE IN COMBATING CYBERCRIME

It is indicated that the current stage of development of civil society is determined by Ukraine's entry to the leading technologically developed countries of the world, to the global information space. Transformation into the information society in all countries is accompanied by the spread of computer (cyber) crimes.

The features of crimes in the sphere of information and telecommunication technologies are studied; attention is paid on the main problems for their identification, detection and investigation. The directions of international cooperation in combating cybercrime, based on international regulations are revealed. Some foreign experience of police units' activities and normative regulation in the Commonwealth and the European Union in this field is highlighted. It is emphasized on the necessity of studying the experience of foreign countries in the organization of the activity of units combating cybercrime. The experience of Canadian police activity in this regard is analyzed. The levels of interaction between operative units of internal affairs agencies for the purpose of operative documentation of crimes in the field of information and communication technologies (interdepartmental, interstate, international) and kinds of cooperation of internal affairs agencies and law enforcement agencies of other states are singled out.

It is noted that improvement of administrative and legal guaranteeing of combating cybercrime in Ukraine should be organized considering national features based on detailed scientific analysis of international law and experience of other countries.

Keywords: *informatization of society, crime in the sphere of information and communication technologies, combating cybercrime, international experience, police, Canada, internal affairs agencies, levels of cooperation, kinds of cooperation.*